International Journal of Electronics,
Communication & Instrumentation Engineering
Research and Development (IJECIERD)
ISSN(P): 2249-684X; ISSN(E): 2249-7951
Vol. 4, Issue 3, Jun 2014, 127-134

TRANS STELLAR
• Journal Publications • Research Consultancy

ADJUSTED TRANSMISSION RANGE REPUTATION BASED LEADER ELECTION FOR IDS IN MANET

SANTOSHKUMAR SABAT[1] & SUJATA KADAM[2]

[1]M.E. Student, Department of Telecommunication, R.A.I.T, Navi Mumbai, Maharashtra, India

[2]Assistant Professor, Department of Telecommunication, R.A.I.T, Navi Mumbai, Maharashtra, India

ABSTRACT

We have proposed an Energy efficient leader election in MANET for Intrusion detection service (IDS). As MANET don't have any centralized controller, the leader election in each cluster becomes very important. The purpose of the elected leader is to serve the IDS for the entire cluster. Our leader election is based on Reputation value and energy level of each node. We have simulated in NS2 environment and shown the comparison of energy consumption or Residual energy of nodes having fixed transmission range with the proposed adaptive energy scheme. Adaptive energy scheme adjusts the range of transmission of each node based on the maximum distance between nodes in each cluster. Energy of each node is conserved as compared to node having fixed transmission range. Thus the leader can serve the cluster for longer duration of life, increasing the percentage of alive nodes, conserving energy of node.

KEYWORDS: Cluster Head, Intrusion Detection System, Leader Election, Mobile Ad-Hoc Network

I. INTRODUCTION

MOBILE ad hoc networks generally consist of mobile battery operated devices that communicate over the wireless network. As we know that intrusion prevention techniques alone, such as encryption and authentication, which are usually a first line of defense, are not sufficient. As the system become more complex, there are also more weaknesses, which lead to more security concerns. Intrusion Detection service (IDs) is to be used as the main line of defense to protect the network from such problems. If the intrusion is detected, a response can be initiated to prevent or minimize damage to the system. Each node may have to carry out its own IDs. However, we observe that at any given instant of time nodes will have different remaining resources, which is to be considered during election of leader. Unless sufficient incentives are provided, nodes might misbehave by acting selfishly and lying about their resources level to not consume their resources for serving others even though they will receive others services. Moreover, even when all nodes can truthfully reveal their resource levels, it remains a challenging issue to elect an energy efficient leader to balance the overall resource consumption. Thus our problem is to elect the most cost efficient leader in the presence of selfish node but as the cost of analysis is private resource information. Node can reveal fake cost of analysis if it's get benefitted by doing this. After getting elected it may not serve for IDS.

Our contribution is we are going to overcome selfish behavior as well as conserve the energy of node using *adaptive energy aware Reputation system model.* Conventionally all the mobile nodes uses the same transmit power. If the transmission ranges of the node decreases or increases, then it must have the dynamicity to adapt the transmission power in order to retain the signal level for that distance. It is enough for each node to have transmission range in order to reach its extreme member in the cluster. By doing so required transmitted power gets reduced and energy efficiency also increases

which increases the lifetime of the node in the network as compared to nodes having fixed transmission range. Thus the node can offer longer duration of intrusion detection service. We have shown using simulation how the adaptive energy scheme is more energy efficient than the fixed range transmission method. We have also shown how the percentage of alive nodes increases and also the residual energy of nodes increases.

The rest of the paper is arranged as follows: section II gives overview of the related work, section III explain the proposed system. Section IV explains the leader election process and explains leader election algorithm, and section V explains simulation scenario and results. Section VI concludes the paper.

II. RELATED WORK

There has been lot of work carried out for efficient leader election in MANET, as too much of resources is wasted for the intrusion detection scheme implementation for every node [8]. Thus the election of leader is prime issue. The election process of leader-IDS can be either random [13] or based on the connectivity [12]. The connectivity model based approach elects a node with a high degree of connectivity even if the node may have little resources left. In both these approaches, some nodes will die faster than others, leading to a loss in connectivity and causing the division of network. Thus energy based leader election will prove to be a better method. In [6] they have proposed an algorithm which elects the node that have high energy and less mobility as cluster head then the cluster head energy level is monitored and then the cluster is altered to increase the lifetime of network. [10] Has shown leader election algorithm which is highly adaptive to topological changes happening arbitrarily in the network. [3] Has shown leader election using mechanism design theory and reputation system model and proved the improvement in behavior of selfish nodes.

III. PROPOSED SYSTEM

We have proposed an adaptive energy aware reputation based leader election model. This model uses the reputation model to overcome the selfish behavior of node by giving them incentives in the form of reputation, so that they will be inspired to honestly participate in the election process by revealing their true cost of analysis. This model also uses adaptive energy scheme i.e. to adapt the transmission power according to the maximum distance of node within the cluster, rather than having conventional fixed transmission range for each cluster.

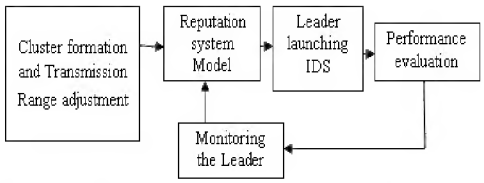

Figure 1: Block Diagram of Proposed System

While forming the cluster the maximum distance between the nodes in the cluster is calculated, the maximum range of distance is set as the transmission range. Then leader election process is initiated based on the initial energy and reputation individual node possess. Once the leader is elected, the elected leader has to perform IDS; based on the performance of the leader the system will update the reputation of the leader. If the leader is not performing above certain threshold performance it will be punished by the reputation system model.

The detection service of node is related to reputation value and also decides the routing priority in the network. We perform a cluster dependent leader election (CDLE) in which the leader is elected after the network is divided into

multiple clusters. Our results indicate that our scheme will increase the lifetime of MANET. Thus, we are able to conserve the overall energy of nodes in cluster by electing energy efficient leader & inspiring the selfish node to honestly participate in election process.

IV. LEADER ELECTION PROCESS

Cost of Analysis Function

As the nodes energy level has to be kept private because then the least cost node has more chance of being attacked. If cost of analysis get decided only based on node's energy level, thus the node's having low energy has no chance to increase their reputation. Thus we design the cost of analysis function based on reputation value & energy level. Each node i has an energy level E_i and the reputation of each node is R_i, the cost of analysis of each node is given by C_i and E_{LID} is the energy level required to launch the IDS.

$C_i = \infty$, if $E_i < E_{LID}$

Otherwise, $C_i = R_i / E_i$

Thus if a node has energy less than E_{LID} it will have infinite cost of analysis.

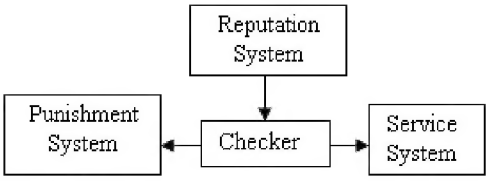

Figure 2: Reputation System Model

This model explains which node to trust. This will inspire the nodes to actively participate in election process. There is also a mechanism which will punish the nodes which are misbehaving by decreasing their reputation. The node that is having high reputation will be most trusted checkers. There are nodes which will monitor the behavior of elected node. They will check the performance of leader in few samples to reduce the overhead of computation. The reputation value is exchanged with nodes in other clusters for service purpose. The checker node exchanges the information of performance behavior of elected node with other to decide about leader election. We set a threshold value of reputation, if the reputation value of node goes below threshold then that node will not be offered any services.

Based on node's reputation value their packet will be forwarded in the network, thus node with low reputation will try to increase their reputation to get more priority in services.

In Presence of Selfish Nodes

The main aim of our work is to inspire selfish node to behave normally during and after the election process. The problem is node may under declare or over declare its cost of analysis C_i.

Under Declare: A node may pretend that it has less cost of analysis than reality but it will not help the node, even though the node will win the election but the node will have to work more than what it is receiving in the form of reputation and even checkers will catch the node.

Over Declare: If a node over declare its cost of analysis then it will never be elected as leader and then it will have no chance to increase its reputation.

Leader Election Algorithm

We have proposed a cost efficient leader election algorithm in the presence of selfish node. Election takes place in the following manner

- Hello message is broadcasted by every node to other node within the cluster.
- Begin election message is broadcasted by each node to all other node within cluster
- Each node sends their cost of analysis to all other nodes.
- Least cost node is elected as leader.
- Leader sends acknowledgement of being elected to others.

Algorithm 1

/* Cluster formation */

- Enter number of mobile nodes.
- Set location of mobile nodes.
- Distance calculation of each node from other node.
- Forming clusters.
- Finding maximum distance in each cluster.
- Based on maximum distance we set the transmission range in each cluster.
- Configuring nodes, setting nodes and its initial energy.

Algorithm 2

/* Begin Election Message */

At $t = T_1$

for (each cluster i)

if (cluster i(node) ! = cluster i (node))

set traffic

else don't broadcast.

Algorithm 3

On expiration of T_1

/* calculation of cost of analysis of each nodes */

At $t = T_2$

Set nodes E_i and R_i

Set cost $C_i = R_i / E_i$

On expiration of T_2

/* Cluster head election */

for (i=0, i< no of nodes)

set $A_i = C_i$

Swap the nodes having least cost in ascending order.

Least cost node is set as selfish node; second least cost node is selected as cluster head.

On expiration of T_3

At $t = T_4$

Cluster head send s being elected message to others. Then to monitor the performance of leader a checker is selected. Set Checker

While (checker ==cluster head || checker ==selfish node)

If the network is attacked by attacker in the form of flooding attack, the cluster head removes the attacker by launching IDS

Reputation update of cluster head happens by launching IDS by seeing this, the selfish node gets inspired to serve the network and to increase its reputation by becoming cluster head.

V. SIMULATION RESULTS

In CDLE setting we perform the analysis of our proposed adaptive energy scheme with fixed transmission range scheme in terms of percentage of alive nodes, residual energy.

Table 1: Simulation Parameter

Parameter	Value
Simulation time	30s
Simulation area	600 x 600
Number of nodes	30,50
Transmission range	500m, adaptive
Movement model	Random way point model
Traffic type	CBR/ UDP
T_{ELECT}	10s
Packet rate	20 packets/sec

Simulation Environment

Initially we assign randomly 30-40 Joules to each node. We show the comparison of adjusted transmission range with fixed transmission range scheme in terms of percentage of alive node and residual energy. Thus proving the proposed

method to be more energy efficient and thus increasing the lifetime of the network. So IDS can be for longer duration.

RESULTS

The comparison of percentage of alive nodes in adjusted range with fixed transmission range is shown for 30 nodes and 50 nodes is shown

Graphs for Time v/s Percentage of alive nodes

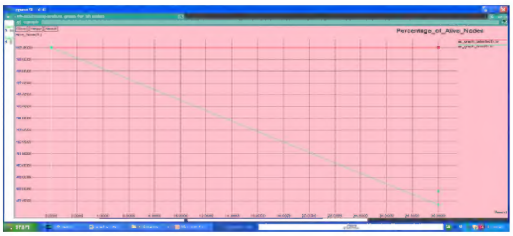

Figure 3 (a): For 30 Nodes

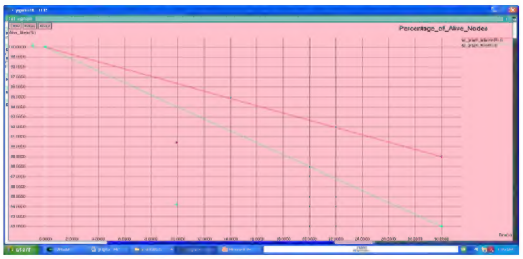

Figure 3 (b): For 50 Nodes

The graph of residual energy of adjusted transmission range and fixed transmission range is shown for 30 nodes and 50 nodes. Thus percentage of alive nodes is more in adjusted range as compared to nodes having fixed transmission range.

Graph for Residual energy v/s Node ID

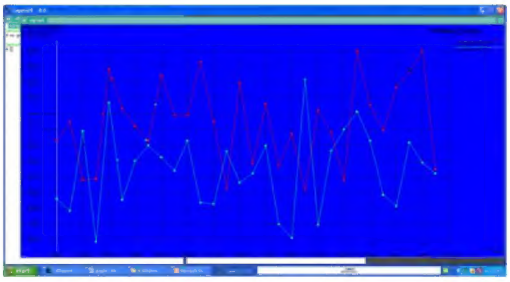

Figure 4 (a): For 30 Nodes

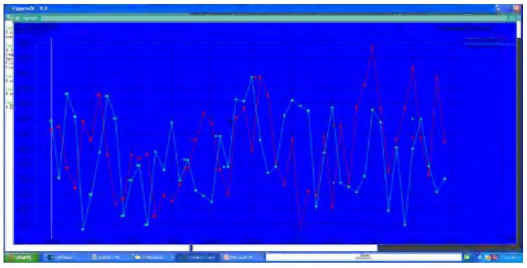

Figure 4 (b): For 50 Nodes

VI. CONCLUSIONS

The selfish behavior of nodes inspired us to propose a Reputation based model with adaptive energy scheme, so that selfish node will be inspired to honestly participate in the election process. We analyzed the performance parameter such as percentage of alive nodes, residual energy and shown that how energy is conserved in adjusted transmission range scheme. Thus our model shows the increase in lifetime of the network, by increasing the percentage of alive nodes and having more residual energy.

ACKNOWLEDGEMENTS

This project work was supported by Electronics and Telecommunication Dept of Dr. D.Y. Patil's group's "Ramrao Adik Institute of Technology", Nerul Navi Mumbai, Maharashtra

REFERENCES

1. T. Sakthivel, S. Vijaybhanu. Rm. Chandrasekaran, "A Novel Leader Based Reputation Approach for Mobile Ad Hoc Networks", IJCA 2012.
2. The Network Simulator (ns-2), "http://www.isi.edu/nsnam/ns/, 2012.
3. Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi, and Prabir Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on dependable and secure computing, vol. 8, no. 1, January-February 2011.
4. Pushpita Chatterjee, "Trust Based Clustering and Secure Routing Scheme for Mobile Ad Hoc Networks", IJCNC 2009.
5. Jochen Mundinger and Jean-Yves Le Boudec "Analysis of a Reputation System for Mobile Ad-Hoc Networks with Liars" Elsevier transaction on performance evaluation, volume 65, issue 3- 4, pp. 212- 226, 2008.
6. Safa. H., Mirza. O., "A Dynamic Energy Efficient Clustering Algorithm for MANETs", Networking and Communications, IEEE International Conference on Wireless and Mobile Computing, 2008.
7. Noam Nisan, Amir Ronen, "Computationally Feasible VCG Mechanism", Journal of Artificial Intelligence, 2007.
8. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer, 2006.
9. Yacine Rebahi, Vicente, E Mujica V and Dorgham Sisalem "A Reputation-Based Trust Mechanism for Ad hoc Networks" proceedings of IEEE symposium on computers and communications, pp. 37- 42, 2005.
10. Sudarshan Vasudevan, Jim Kurose, Don Towsley, "Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks", Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP'04).
11. Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2003.
12. Challenges in Intrusion Detection for wireless Ad-hoc Networks, Y. Paul Brutch & Kelvin Ko, Network associates Laboratory.

13. Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", ACM/Kluwer Wireless *Networks Journal (ACM WINET), Vol. 9, No. 5, September,2003*